REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
27-05-2008

2. REPORT TYPE
FINAL

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE

Operational Command and Control of Joint Task Force Cyberspace Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Mike Elliot, LCDR, USN

Paper Advisor (if Any): Stephanie Helm, CAPT, USN

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department

Naval War College

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT: Command and Control (C2) is one of the most, if not the most, important Operational Function for a Joint Force Commander (JFC). History is replete with examples where inadequate or overly complicated C2 has adversely impacted a military's ability to attain their operational objectives. According to Dr. Milan Vego, to successfully attain their objectives, JFCs are best served by adhering to the time tested tenets of Operational C2. Throughout history, advances in technology and the military's incorporation of them have drastically altered the face of war (e.g. airplane in WWII). Today, the military is in the midst of a technological revolution due to the proliferation of the internet and other network-based communications - often referred to as cyberspace - and its inclusion into nearly every aspect of operations. Cyberspace provides the military an additional and unique method to operationally survey, recon, and strike enemy forces, while providing a means to operationally sustain and protect its own forces. The Joint community has not yet developed doctrine on how to operationally C2 cyberspace operations. Current dialogue and initiatives regarding C2 of cyberspace operations are embedded in the larger discussion concerning the C2 of Information Operations (IO). Many of these previous efforts have analyzed IO as a collective whole rather than analyzing each core capability, or viewed cyberspace solely as a sub-element of the information environment rather than viewing it as a unique domain. This paper focuses solely on analyzing and determining the optimal method in which to operationally C2 cyberspace operations in a Joint Task Force (JTF). Finally, this paper recommends that a Joint Functional Cyberspace Component Commander (JFCCC) be formerly incorporated into Joint Doctrine for the purposes of operationally commanding and controlling cyberspace operations in current and future campaigns and operations.

15. SUBJECT TERMS
Cyberspace; Command and Control (C2); Information Operations (IO); Computer Network Operations (CNO); Electronic Warfare (EW); Global Information Grid (GIG)

16. SECURITY CLASSIFICATION OF:

a. REPORT
UNCLASSIFIED

b. ABSTRACT
UNCLASSIFIED

c. THIS PAGE
UNCLASSIFIED

17. LIMITATION OF ABSTRACT

18. NUMBER OF PAGES
35

19a. NAME OF RESPONSIBLE PERSON
Chairman, JMO Dept

19b. TELEPHONE NUMBER *(include area code)*
401-841-3556

NAVAL WAR COLLEGE

Newport, R.I.

OPERATIONAL COMMAND AND CONTROL OF JOINT TASK FORCE CYBERSPACE OPERATIONS

by

Michael C. Elliot

Lieutenant Commander / U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: ___________________________

27 May 2008

Abstract

Command and Control (C2) is one of the most, if not the most, important Operational Function for a Joint Force Commander (JFC). History is replete with examples where inadequate or overly complicated C2 has adversely impacted a military's ability to attain their operational objectives. According to Dr. Milan Vego, to successfully attain their objectives, JFCs are best served by adhering to the time tested tenets of Operational C2. Throughout history, advances in technology and the military's incorporation of them have drastically altered the face of war (e.g. airplane in WWII). Today, the military is in the midst of a technological revolution due to the proliferation of the internet and other network-based communications - often referred to as cyberspace - and its inclusion into nearly every aspect of operations. Cyberspace provides the military an additional and unique method to operationally survey, recon, and strike enemy forces, while providing a means to operationally sustain and protect its own forces. The Joint community has not yet developed doctrine on how to operationally C2 cyberspace operations. Current dialogue and initiatives regarding C2 of cyberspace operations are embedded in the larger discussion concerning the C2 of Information Operations (IO). Many of these previous efforts have analyzed IO as a collective whole rather than analyzing each core capability, or viewed cyberspace solely as a sub-element of the information environment rather than viewing it as a unique domain. This paper focuses solely on analyzing and determining the optimal method in which to operationally C2 cyberspace operations in a Joint Task Force (JTF). Finally, this paper recommends that a Joint Functional Cyberspace Component Commander (JFCCC) be formerly incorporated into Joint Doctrine for the purposes of operationally commanding and controlling cyberspace operations in current and future campaigns and operations.

Contents

List of Illustrations

INTRODUCTION

The Operational Function of Command and Control (C2) is one of the most, if not the most, important Operational Function for a Joint Force Commander (JFC) because “it is the principal means by which the [Joint Force] commander sequences and synchronizes the actions and activities of both military and nonmilitary sources of national power in a given theater.”[1] History is replete with examples where non-existent, inadequate, excessive or overly complicated Operational C2 has adversely impacted a military’s ability to attain their operational objectives or unduly increased risk to the force and/or the mission. In order to successfully attain their objectives, JFCs are best served by adhering to the time tested tenets of Operational C2 - simplicity, flexibility, unity of effort (UoE), integration, continuity, homogeneity, balance, and stability - when designing their Joint Force C2 structure.[2]

Advances in technology and the U.S. military’s incorporation of these new technologies into its capability sets has drastically altered the manner in which future wars would be conducted. One of the most significant technological advances was the invention of the airplane. The integration of the airplane into the military completely changed the face of war by providing another manner in which to operationally move, maneuver, and sustain forces. Furthermore, it offered an additional method in which to operationally survey, recon, and strike enemy forces, while providing another means to operationally protect its own forces. Although the addition of the aircraft, and air forces, to the military was welcomed, the manner in which they were to be operationally commanded and controlled was a highly contentious issue, which was eventually resolved through the development of Joint Doctrine for the C2 of Air Operations.[3]

Today, the military is in the midst of a similar situation as a result of the advent and proliferation of the internet and other network-based communications - often referred to as cyberspace - and its inclusion into nearly every aspect of operations. Analogous to the airplane, the incorporation of cyberspace into the military has completely changed the face of war. Military forces cannot operationally move and maneuver in cyberspace in a physical manner; however, cyberspace provides the military an additional and unique method to operationally survey, recon, and strike enemy forces, while providing a means to operationally sustain and protect its own forces. Similar to the airplane, the military services have harnessed the advantages of cyberspace by integrating its capabilities into in all facets of operations. However, unlike Air Operations, the Joint community has not yet developed, nor is it currently developing, Joint Doctrine for the purpose of advising current and future JFCs how to best Operationally C2 cyberspace operations.[4]

Current dialogue and initiatives regarding C2 of cyberspace operations are embedded in the larger discussion concerning the Operational C2 of Information Operations (IO), mainly because Computer Network Operations (CNO) and Electronic Warfare (EW) are doctrinally two of the five core capabilities of IO.[5] In recent years, military professionals have written extensively on the issue of Operational C2 of IO, including several who have recommended that Joint Doctrine provide provisions for the establishment of a Functional Component Commander (FCC) who would be responsible for the Operational C2 of IO.[6] Additionally, several of today’s standing Joint Task Forces (JTFs) have had similar discussions, and even conducted Command Post and Field Training Exercises with a variety of constructs for the Operational C2 of IO, to include the Joint Force Information Operation Component Commander (JFIOCC) and/or the JTF Commander (CJTF) retaining C2 of IO.[7] Although these are valid and important discussions, the critical flaw has been two-fold, first, many of these studies analyzed IO as a collective whole, rather than individually analyzing each core capability, second, they viewed cyberspace solely as a sub-element of the information environment, rather than viewing it as a unique domain.

Unlike these previous efforts, this paper focuses solely on analyzing and determining the optimal method in which to C2 cyberspace operations in a JTF construct, not the entire spectrum of IO. In order to determine the optimal operational level C2 construct, this paper will first define what constitutes cyberspace and explain how its attributes cause difficulties with the traditional "Theater Structure and Levels of War"[8] construct. Second, it will explain what cyberspace does for the JTF and discuss the adverse impact to the achievement of operational objectives that can occur if the requisite focus of effort is not applied to cyberspace operations. Third, the paper will explain what cyberspace forces are, where they are located in a JTF, how they are traditionally task-organized, and it will address the significant problems this task-organization construct causes for cyberspace operations. Fourth, the paper will present three possible constructs for the Operational C2 of cyberspace operations: U.S. Strategic Command (USSTRATCOM), JTF, and FCC, and analyze these constructs against three of noted operational art theorist Dr. Milan Vego's tenets of Operational C2 – simplicity, UoE, and homogeneity. Finally, based on the results of this analysis, this paper will recommend that a Joint Functional Cyberspace Component Commander (JFCCC) be formerly incorporated into Joint Doctrine for the purposes of operationally command and controlling cyberspace operations in current and future campaigns and operations.

[redacted]

MEDIUM – ENVIRONMENT – DOMAIN – DIMENSION (MEDD)

Current Joint Doctrine does not define the terms medium, environment, domain or dimension (heretofore referred to as "MEDD"), yet, nearly all military professionals are familiar with and readily use these terms.[9] This is not merely an issue of semantics, but a significant distinction because the military customarily task-organizes its services and joint forces along MEDDs. The Departments of the Navy, Army and Air Force are primarily responsible for organizing, manning, training, and equipping of forces to operate in the maritime, land and air MEDDs respectively.[10] Additionally, during joint campaigns and operations, our military forces are similarly task-organized to operate in the maritime, land, and air MEDDs through the establishment of service or joint FCCs.[11]

HOW ARE MEDDS CHARACTERIZED?

To answer this question, we look at current Joint Doctrine, which characterizes MEDDs through the concept of the Operational Environment, "the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. It encompasses physical areas and factors (of the air, land, maritime, and space domains) and the information environment."[12] Furthermore, Joint Doctrine defines the information environment as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."[13] The information environment is sub-divided into three dimensions - physical, informational, and cognitive.[14] Quite strikingly, cyberspace is not included in the concept of the Operating Environment nor specifically included in any of the three sub-component definitions of the information environment. Additionally, cyberspace is neither addressed nor discussed in JP 3-0, *Joint Operations*, or JP 3-13, *Joint Doctrine for IO*, but only defined in JP 3-13 as "the notional environment in which digitized information is communicated over computer networks."[15] Furthermore, the current Quadrennial Defense Review and National Military Strategy (NMS), although neither specifically define cyberspace, both refer to it as a domain, and the NMS further characterizes cyberspace as one of the four global commons, on par with international airspace, waters, and space.[16]

WHAT IS CYBERSPACE?

Clearly understanding what cyberspace is and is not, is essential to determining the optimal method of commanding and controlling cyberspace operations. Although JP 3-0, JP 3-13, and the current QDR and NMS classify cyberspace as an environment or domain, none of these documents define its attributes or characteristics with any fidelity. One Joint Publication, JP 2-01.3, *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*, indentifies the attributes and characteristics of cyberspace as "composed of computer hardware, networks, software, data, procedures, and human operators."[17] Moreover, the Air Force recently characterized cyberspace as "the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked information systems and associated physical infrastructures."[18] Both definitions provide some fidelity to cyberspace, but leave much to be desired, especially in regard to cyberspace's relationship with the other domains and the information environment.

For the purposes of this paper, cyberspace is considered a homogeneous, physical domain which resides inside the collective boundaries of the traditional physical domains - air, land, maritime and space, and co-exists in some regions with these other traditional physical domains much like the co-existence of the air, land, and maritime domains in the littoral region, see Figures (1) and (2).[19] Furthermore, cyberspace is defined as the aggregation of all Electro-Magnetic (EM) equipment located in the physical domains that is networked together by hard-line (fiber-optics, wire, etc.) and air-gap (via the EM spectrum) connections for the purposes of storing, modifying, and exchanging information in the form of data through interaction with both animate and inanimate entities in the physical domains to support the human cognitive dimension and influence electro-mechanical objects in all of the physical domains. It is critical to highlight that in this definition, cyberspace relies not only on hard-line connections facilitated by the EM spectrum (electrical impulses and optics) to exchange data (the realm of CNO), but is also dependent on air-gap connections facilitated by the EM spectrum (infrared and radio waves) to exchange data (the realm of EW).

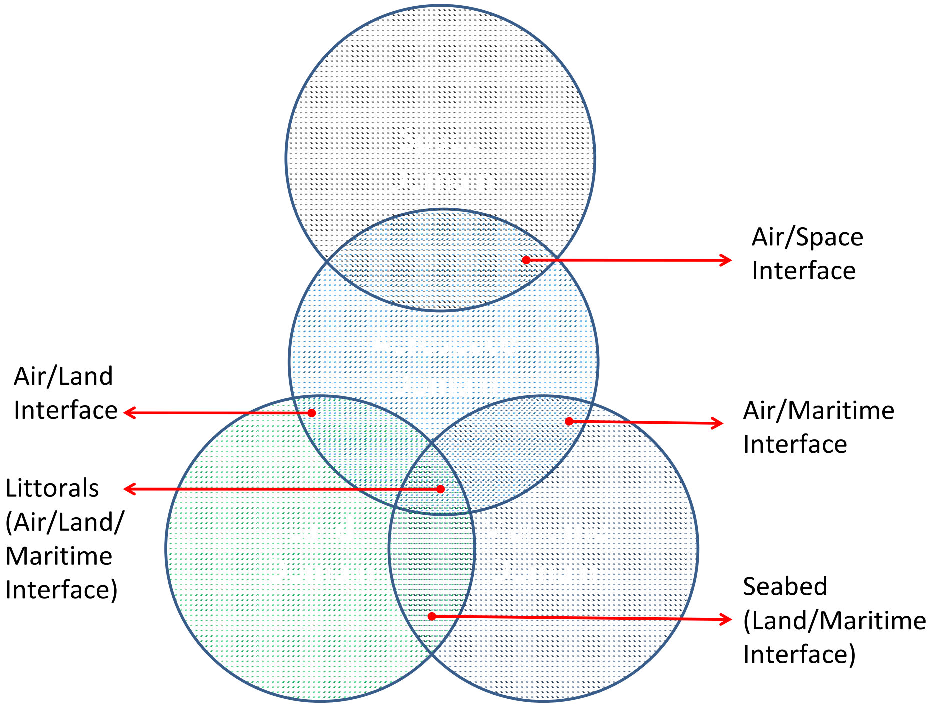

Figure 1: Physical Environment

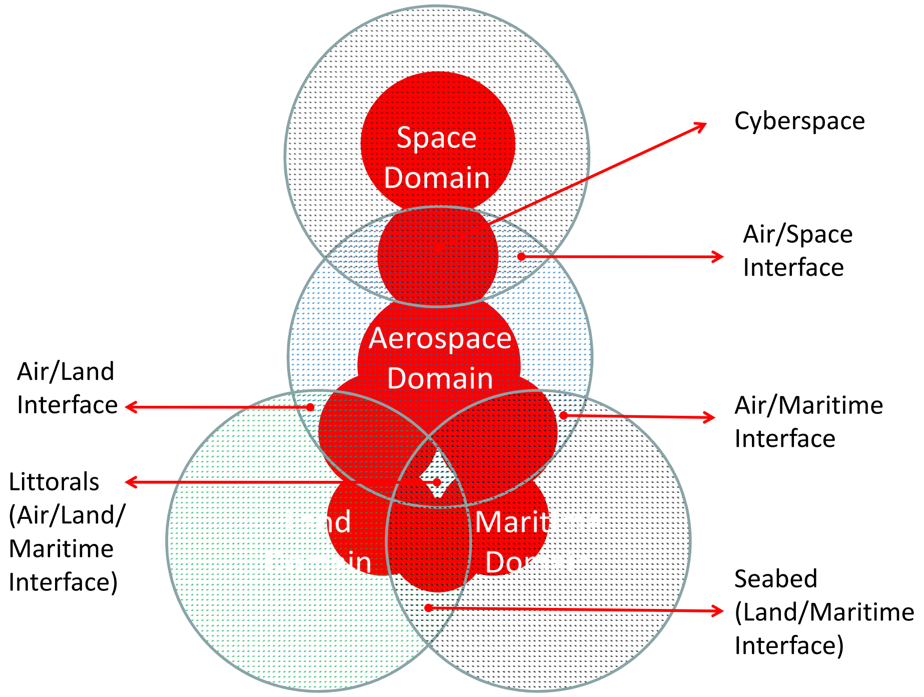

Figure 2: Physical Environment (to include Cyberspace)

THEATER STRUCTURE AND LEVELS OF WAR

Per Dr. Vego's "Theater Structure and Levels of War" concept, a "theater should be militarily organized to ensure the most favorable conditions for the employment of one's forces across the entire spectrum of conflict."[20] Furthermore, he states that "the theater has to be divided into a number of geographically based areas to ensure the most effective employment of one's military and non-military sources of power" and that "the theater and its subdivisions are the very basis for establishing and maintaining tactical, operational, and strategic levels of command or command echelons."[21]

These concepts apply easily to the land and maritime domains for two reasons, first, boundaries can be established to differentiate between physical regions in these domains, second, the speed of friendly and enemy forces operating in these domains is relatively slow, which permits moderately easy transfer of friendly forces between and among the three levels of command, and the tracking of enemy forces.[22] Although enemy and friendly forces operating in the air and space domains travel at speeds that are orders of magnitude higher than forces operating in the land and maritime domains, Dr. Vego's concept still applies to the air and space domains because the movement of enemy or friendly forces in the space domain is known in advance due to orbital physics. That is, objects operating in space (satellites and spacecraft) rely on the earth's gravitational pull to propel them thru space. Moreover, technology, to include RADAR, imagery, and signals intelligence, enables the tracking of both friendly and enemy forces operating in the air and space domains. For these reasons, designating tactical, operational, and strategic levels of command in these domains is possible and transferring forces between and among these levels is relatively simple.

However, Dr. Vego's concept does not easily apply to cyberspace because the speed of both friendly and enemy forces, ranging from the speed of sound to the speed of light, makes tracking them difficult to nearly impossible. A cyberspace force can move from one side of the globe to the other in milliseconds, thus theoretically moving from a tactical to strategic level of command. Although geographical regions could nominally be established for cyberspace, whether equating to the boundaries established for the land, air, or maritime domains, or to boundaries established by linking communication nodes, for the above reasons the nature of cyberspace presents difficulties in designating levels of command.

[redacted]

WHAT DOES CYBERSPACE DO FOR THE JTF?

We've established what cyberspace is, but what does it actually do for the JTF at the operational level of war? First, recall that Operational C2 is recognized as "the principal means by which an operational commander sequences and synchronizes joint force activities in peacetime and orchestrates use of military and nonmilitary sources of power to accomplish assigned strategic objectives in war."[23] Then, consider that "C2 cannot be successful without a well-developed, highly efficient, and survivable theater-wide [and area of operations-wide] command, control, communications, and computer (C4) system."[24]

The C4 system is composed of three principal components - command, control, and the C2 system. Command is "the authority and responsibility for effectively using available resources for planning the employment of, organizing, directing, and coordinating military forces for the accomplishment of assigned [operational] missions."[25] Control is "inherent in command, and is used to regulate forces and [Operational] functions to execute the commander's intent."[26] Finally, the C2 system comprises the "facilities, equipment, communications, procedures, and personnel essential to a [Joint Force] commander for planning, directing, and controlling operations of assigned and attached forces pursuant to the [operational] mission [and objectives] assigned."[27] Thus, the C2 system is the mechanism which enables the CJTF to operationally command and control his forces, without this system modern day campaigns and operations would not be possible.

Furthermore, the foundation for today's C2 system is the Global Information Grid (GIG), "the DOD's globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to joint forces."[28] The GIG "includes all [military] owned and [commercially] leased communications and computing systems and services, software, data, security services, and other associated services necessary to achieve information security" and "provides interfaces to multination and non-DOD users and systems."[29] Similar to cyberspace, it is critical to understand that the GIG relies not only on hard-line connections facilitated by the EM spectrum to exchange data (the realm of CNO), but is also dependent on air-gap connections facilitated by the EM spectrum to exchange data (the realm of EW), see Figure (3).[30] Since the GIG is connected to other global and globally connected information systems, it is part of the overall cyberspace domain. Therefore, events that occur in cyberspace can impact, positively or negatively, the JTF's C2 system, which would in turn directly impact the JTF's ability to C2 its subordinate forces.

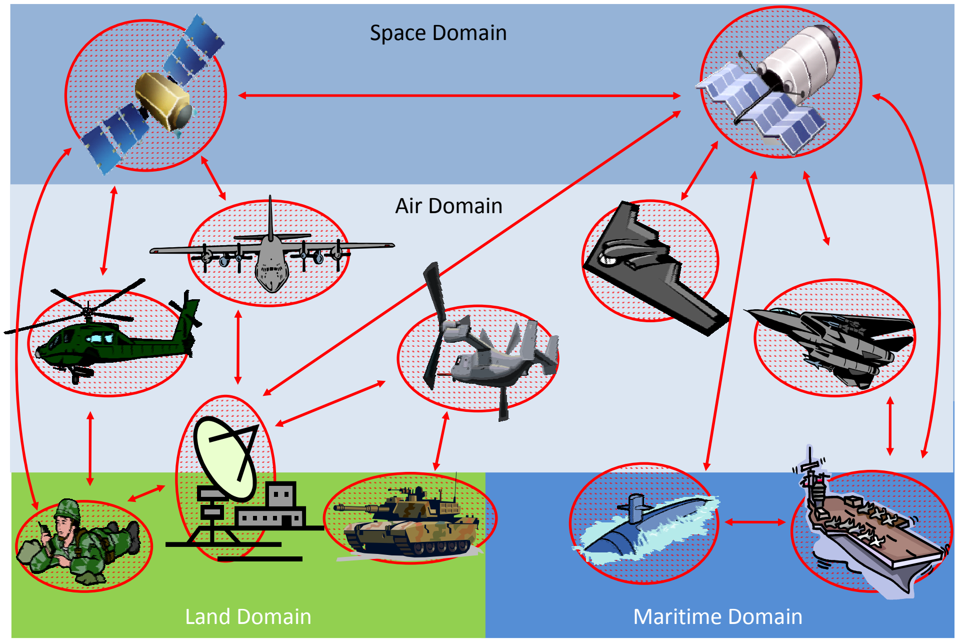

Figure 3: Global Information Grid (GIG): Red Circles and Lines represent the Military portion of cyberspace (GIG).

In addition to enabling Operational C2, the Operational Functions of "intelligence, fires, logistics, and protection all depend on responsive C4" and, thus the C2 system.[31] JP 2-0, *Joint Intelligence*, explains that "an intelligence sharing architecture is integral to all [operational level] intelligence operations and that this architecture functions over the GIG"; therefore, actions that occur in cyberspace can directly impact Operational Intelligence.[32] Per JP 3-9, *Joint Fires*, [Operational] fires require "the coordinated interaction of all elements of the fire support system," which includes the "target acquisition, C2, and attack/delivery systems."[33] Similar to the intelligence sharing architecture, since the fire support systems are part of the GIG, actions in cyberspace can directly impact Operational Fires.

Operational Protection involves the integration of multiple components to preserve "the effectiveness and survivability of military and non-military sources of power."[34] These components include collecting intelligence for indications and warning, protection of information systems, ballistic missile defense, and several others, all of which are dependent on the C2 system, and thus the GIG, to function individually and collectively.[35] Finally, the critical enabler for Operational Logistics is the "implementation of [an] end-to-end support capability by integrating existing information technologies and logistic automated information systems," which ensures that a campaign or operation can be adequately supported and logistically sustained.[36] Therefore, Operational Protection and Logistics may also be adversely impacted by actions in cyberspace because of their reliance on the GIG.

The above discussion clearly demonstrates that five of the six Operational Functions of war - C2, intelligence, fires, logistics, and protection - are highly dependent on the access to and actions that occur in the cyberspace domain because the GIG is connected to cyberspace. If the CJTF does not place the requisite emphasis on the maintenance, operation, and defense of his "portion" of the GIG and its interaction with cyberspace, he places at risk his ability to conduct one or all of these Operational Functions; and ultimately jeopardizes the likelihood of achieving his assigned strategic and operational objectives.[37]

Besides enabling the JTF's Operational Functions, cyberspace also enables the Operational Functions of other nation-state militaries and non-state actors, some of whom are currently or may become our adversaries. Therefore, cyberspace provides a mechanism in which to attack one or more of an adversary's Operational Functions, and possibly directly or indirectly attack the adversary's Center of Gravity (CoG). If the CJTF does not place the requisite emphasis on understanding the adversary's use of and reliance on cyberspace, and does not leverage his capabilities that can strike an enemy in the cyberspace domain, he may miss or severely limit the opportunity to achieve his strategic and operational objectives.

[redacted]

WHAT ARE CYBERSPACE FORCES?

Clearly understanding what constitutes cyberspace forces is critical to determining the appropriate manner in which joint force cyberspace operations should be commanded and controlled because "C2 encompasses the exercise of authority and direction by a commander over assigned and attached forces in the accomplishment of the mission [objectives]."[38] Although cyberspace has only recently been formally recognized as a domain, both the joint community and services have maintained cyberspace forces for quite some time, and have recently focused efforts on increasing the size and quality of some of these forces. So, what is a cyberspace force? Once again, none of the Joint or Service Publications provide a formal definition, although Air Force Doctrine Document 2-8, *Command and Control*, cites the term "cyberspace forces" in several instances, though without providing a formal definition.[39]

Before defining what constitutes a cyberspace force, it is essential to understand what constitutes a military force. Per JP 1-02, a military force is "an aggregation of military personnel, weapon systems, equipment, and necessary support, or combination thereof."[40] Considering this definition, this paper's definition of cyberspace, and the concept of the GIG, a cyberspace force is defined as - the aggregation of military personnel, hardware, software, and necessary support that manage, maintain, operate, and defend the GIG and exploit and attack targets in cyberspace, to include adversary GIG-equivalent systems. This definition clearly delineates between those forces (land, maritime, air, and space), who use the GIG/cyberspace as a mechanism to support the performance their primary mission - operations in the land, maritime, air, and space domains, and those forces (cyberspace forces), who operate inside the GIG/cyberspace to exploit and attack adversaries.

Cyberspace forces can be separated into three groups - Communications, CNO, and EW forces. Although these forces are categorized as cyberspace forces because they operate inside cyberspace, they are routinely located in and perform missions in support of the other physical domains. The division into this construct is based on the mission and function that each performs. Communications forces consist of two groups: Information Management (IM) and Information Assurance (IA) forces. IM forces "enable the provision of relevant information to the right person at the right time in a useable format for situation awareness and decision making."[41] IA forces "ensure the security of information and the communications system through information protection, intrusion/attack detection and effect isolation, and incident response to restore information and system security."[42]

CNO forces consist of Computer Network Defense (CND), Exploitation (CNE), and Attack (CNA) forces. CND forces take actions through the use of computer networks "to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks [the GIG]."[43] CNE forces conduct "enabling operations and intelligence collection … through the use of computer networks [the GIG] to gather data from target or adversary information systems of networks [adversary's GIG-equivalent system]."[44] CNA forces take actions "through the use of computer networks [the GIG and cyberspace] to disrupt, deny, degrade, or destroy information resident in [adversary] computers and computer networks, or the computers and networks themselves."[45]

EW forces consist of Electronic Support (ES), Protect (EP), and Attack (EA) forces. EA forces take actions through the use of "EM energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying adversary combat capability."[46] EP forces conduct actions to "ensure the friendly use of the EM spectrum."[47] ES forces take actions "to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated EM energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations."[48]

WHERE ARE CYBERSPACE FORCES LOCATED IN A JTF?

We have established what cyberspace forces are, but where are they located in a JTF, and to whom do they belong? In order to answer these questions we will look at a typical JTF organization. A JTF normally consists of several subordinate service or joint components that the CJTF designates "to integrate planning; reduce [his] span of control; and/or significantly improve combat efficiency, information flow, UoE, weapon systems management, component interaction, or control over the scheme of maneuver."[49] These components are traditionally designated along the physical domains, through the establishment of Joint FCCs for the Land, Air, and Maritime components (JFLCC, JFACC, and JFMCC) and the Space Control Authority (SCA).[50] JTFs establish other subordinate components to plan, coordinate, and synchronize operations that are non-physical domain specific, such as psychological, special, and civil-military operations.[51]

However, JTFs do not normally designate a specific service or joint FCC to plan, coordinate, and monitor operations in the cyberspace domain, as evidenced by the fact that Joint Doctrine does not provide provisions for such.[52] Rather, these responsibilities are dispersed throughout both the JTF headquarters staff and the subordinate FCCs and/or Task Forces (TFs). In a JTF headquarters, two staff elements, the Directorate for Communications (J6) and the Directorate for IO (J39), together maintain collective responsibility for planning, coordinating, and monitoring overall JTF cyberspace operations.

Principally, the J6 “ensures that an adequate and effective communications system is available to support the joint force C2 system,”[53] and mostly employs assigned and attached IM and IA forces to perform this mission. Besides other responsibilities, the J39 “coordinates [the] integration and synchronization of CNO [and EW] with other IO capabilities and deconflicts CNO [and EW] with other staff directorates,”[54] to include the J6, in order to defend the JTF’s “portion” of the GIG while exploiting and attacking adversary information and information systems, through the employment of assigned and attached CNO and EW forces. In addition to this division of labor arrangement at the JTF headquarters, these arrangements similarly exist at the each subordinate FCC and/or TF, especially in the case of EW where each FCC often has its own EW forces.

The significant issue that occurs as a result of this cyberspace force task-organization arrangement is suboptimal UoE. UoE is the “coordination and cooperation toward common objectives”[55] which “can be achieved either through Unity of Command (UoC) or through cooperation.”[56] According to Dr. Vego, “the highest degree of effectiveness is ensured by having UoE though UoC” and “failure to establish UoC results in a state of divided command,” which “has probably been the cause of more defeats, and disasters than any other factor” in the history of war.[57] As previously discussed, cyberspace provides a mechanism in which to attack one or more of an adversary’s Operational Functions, and possibly directly or indirectly attack the adversary’s CoG; and offers an adversary the ability to do the same to friendly forces. According to Dr. Vego, “without [UoC] the [JTF] cannot bring all available forces to bear against the enemy at the decisive place and time” either to defend or attack.[58] Current cyberspace task-organization in a JTF requires that UoE for cyberspace operations be conducted in a cooperative, rather than a UoC manner.

[redacted]

POSSIBLE CYBERSPACE C2 MODELS

Now that we understand what cyberspace is, what it does for the JTF, what cyberspace forces are, and the significant problem with the current cyberspace force task-organization, we can begin to develop a recommendation for how a JTF should operationally command and control cyberspace operations. We will do this by examining three possible types of cyberspace C2 models – STRATCOM, JTF, and FCC, and analyze these constructs against Dr. Vego's tenets of Operational C2.

The first is the STRATCOM construct, where STRATCOM is responsible for the C2 of cyberspace operations and retains Operational Control (OPCON) of cyberspace forces.[59] The second is the JTF construct, where the JTF is responsible for the C2 of cyberspace operations and is delegated OPCON of cyberspace forces. The last is the FCC construct, where a FCC, nominally, the Joint Force Cyberspace Component Commander (JFCCC) is responsible for the C2 of cyberspace operations and is delegated OPCON of cyberspace forces. These constructs have not been arbitrarily chosen; they have actually been discussed and postulated in real-world JTFs and among the Regional Combatant Commanders.[60] Due to length limitations, this paper analyzes these C2 models against only three of Dr. Vego's Operational C2 tenets – simplicity, UoE, and homogeneity.[61] In the below analysis, a grade of HIGH, MEDIUM, or LOW is assigned to each of these tenets for the three C2 constructs based on how well, or poorly that particular tenet is satisfied.

<u>Simplicity</u>: The JFCCC model earns a HIGH grade in simplicity because it has the most clear and straightforward CoC. The operational level cyberspace forces report to the

JFCCC, who reports directly to the JTF. Although not as clear and straightforward as the JFCCC model, the JTF model earns a MEDIUM grade. In this model, the operational forces report directly to the JTF, without an intermediary operational commander, which is cumbersome because in addition to performing his primary function of sequencing and synchronizing the actions and activities of all the FCCs, the CJTF must himself perform the duties of a FCC. The least simplistic of the three is the STRATCOM model, because its CoC is extremely awkward and cumbersome. In this model, STRATCOM is a supporting commander to the JTF, which although awkward, is not wholly unrealistic. The issue which arises goes back to the discussion on the "Theater Structure and Levels of War." The CJTF is concerned with the smaller Theater of Operations and achieving his assigned operational objectives, however, STRATCOM is concerned with both supporting the CJTF, and achieving his own national strategic objectives; thus this model earns a LOW grade.

UoE: The JFCCC model earns a HIGH grade in UoE because in this model a single commander is controlling all the operational forces that are assigned to the mission of managing, maintaining, operating, and defending the JTF's "portion" of the GIG; in addition to exploiting and attacking targets in cyberspace and adversary GIG-equivalent systems. Additionally, the JTF model earns a HIGH grade in UoE for these very same reasons, although the problems discussed in the simplicity tenet still exist. In both of these models, not only is UoE maximized for cyberspace operations, but UoE is maximized for all of the JTF operations because a single commander is controlling all of the operational forces – land, air, maritime, space, and cyberspace, whose actions are coordinated and synchronized by the CJTF to achieve the operational objective(s). However, in the STRATCOM model, UoE is not preserved for all JTF operations, thus this model receives a MEDIUM grade. This model does satisfy UoE for cyberspace operations because STRATCOM would retain OPCON of cyberspace forces, but, overall UoE would not exist since the other operational forces – land, air, maritime, and space would be controlled by the JTF.

Homogeneity: The JFCCC model earns a MEDIUM-HIGH grade in homogeneity because in this model all the functions required to accomplish the mission of managing, maintaining, operating, and defending the JTF's "portion" of the GIG; in addition to exploiting and attacking targets in cyberspace and adversary GIG-equivalent systems are grouped into one command. However, not all the cyberspace forces in the JTF would necessarily be assigned or attached to the JFCCC. As previously discussed, cyberspace enables the JTF to perform each of his six Operational Functions. This also holds true for each FCC; therefore, each FCC would require its own attached or assigned cyberspace forces, principally IM, IA, CND, and EW forces. The JFCCC would consist of all CNA and CNE forces, and the remainder of those IM, IA, CND and EW forces not attached or assigned to the other FCCs and the JTF. In the JTF model, all the functions required to accomplish the mission of maintaining, operating, and defending the JTF's "portion" of the GIG; in addition to exploiting and attacking targets in cyberspace and adversary GIG-equivalent systems are grouped into one command. Similar to the JFCCC model, not all the cyberspace forces would be attached or assigned to the JTF because some IM, IA, CND, and EW forces would need to reside at each FCC to enable performance of their mission specific Operational Functions. However, the JTF model earns a slightly lower grade of MEDIUM because of the same issues discussed in simplicity, the JTF must function as both the overall operational commander and a FCC. Although the STRATCOM model would have all functions – maintain, defend, exploit, and attack, at the same command, each FCC and the JTF would need its own assigned or attached IM, IA, CND, and EW forces to enable their Operational Functions. This model earns a MEDIUM-LOW grade because all CNA/CNE forces would reside at a command responsible for both its own national and theater-strategic objectives, while also tasking these forces to support the JTF's operational objectives.

The analysis of these three possible cyberspace C2 models – STRATCOM, JTF, and JFCCC, through the lens of Dr. Vego's Operational C2 tents clearly shows that the JFCCC model is the most effective and efficient method of commanding and controlling cyberspace forces at the operational level of war. The results of this analysis are presented in Table (1).

C2 Model	Simplicity	Unity of Effort	Homogeneity
STRATCOM	LOW	MEDIUM	MEDIUM-LOW
JTF	MEDIUM	HIGH	MEDIUM
JFCCC	HIGH	HIGH	MEDIUM-HIGH

Table 1: Operational C2 tenet analysis

CONCLUSION

The development, proliferation, and integration of networked-based computer and information systems into today's military force structure and operating concepts has arguably made the U.S. military the most potent and capable combat force in the history of the world. However, one of our greatest strengths has perhaps become our single greatest vulnerability. As presented in this paper, five of the Operational Functions - C2, Intel, Fires, Protect, and Logistics directly rely on the availability, reliability, and security of the GIG. Since the GIG is connected to cyberspace, actions that occur in cyberspace can adversely impact the ability of the JTF to perform each or all of its Operational Functions, which may in turn prohibit the CJTF from achieving his operational objective(s). Additionally, since cyberspace enables the Operational Functions of some, if not all, of our adversaries, it provides a mechanism to attack an adversary's Operational Functions, and possibly directly or indirectly, their CoG(s).

Therefore, if JTFs want to achieve their assigned operational objectives, they must place an emphasis on maintaining, operating, and defending their “portion” of the GIG, while understanding the adversary’s GIG-equivalent system and cyberspace. Today’s JTFs are equipped with cyberspace forces that are capable of performing these functions, and tomorrow’s JTFs will be provided more capable cyberspace forces, especially in regard to exploit and attack capabilities. The question that confronts us today is do we perform these critical functions in a disjointed and sometimes duplicative manner, indicative of today’s JTF cyberspace force task-organization, or do we optimize these efforts to ensure mission success?

Optimization is best achieved by grouping the majority, but not all, of these forces together, and assigning a single commander to plan, coordinate, monitor and redirect their actions to support the JTF’s Concept of Operations (CONOPs). As evidenced by Dr. Vego’s Operational C2 tenets of simplicity, UoE, and homogeneity, the best method of achieving optimization of JTF cyberspace operations would be through the establishment of a JFCCC, who would be directly responsible to the CJTF for all operational-level cyberspace operations.

END NOTES

[1] Milan N. Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: Naval War College, 2007), VIII-20.

[2] Ibid., VIII-13 – VIII-18. "To ensure the most effective employment of one's forces in the accomplishment of their assigned objectives or tasks, certain cardinal rules or tenets should be following in establishing the command organization. These tenets are not a checklist that can be applied fully or in a rigid manner. They should be applied flexibly and with common sense."

[3] Chairman, U.S. Joint Chiefs of Staff, *Command and Control for Joint Air Operations*, Joint Publication (JP) 3-30 (Washington, DC: CJCS, 5 June 2003, i. "This publication provides fundamental principles and doctrine for the command and control of joint air operations throughout the range of military operations."

[4] No current Joint Doctrine Publications specifically address or discuss C2 of Cyberspace Operations as evidenced by a review of the current versions of JP 1-02 (*Department of Defense Dictionary of Military and Associated Terms*, JP 3-0 (*Joint Operations*), JP 3-13 (*Information Operations*), and JP 3-33 (*Joint Task Force Headquarters*). Additionally, the most current Joint Doctrine Update in Joint Forces Quarterly (Issue 49, 2nd Quarter 2008) does not indicate that any Joint Publications are being specifically developed for Computer Network Operations (CNO) or for the C2 of Joint Cyberspace Operations.

[5] Chairman, U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13 (Washington, DC: CJCS, 6 February 2006), x. "IO consists of five core capabilities which are: PSYOP, MILDEC, OPSEC, EW, and CNO."

[6] John M. Myers, LCDR, USN "Operational Command and Control for Information Operations" (research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2006), 1; and Mark W. Maiers and Timothy, L. Rahn, "Information Operations and Millennium Challenge." *Joint Forces Quarterly*, no. 35 (Autumn 2004): 87. LCDR Myers Research Paper: This paper suggests that IO should be assigned to a permanent organization through the creation of a Theater Information Operations Command (TIOC). During normal operations, the TIOC would be OPCON to the combatant commander. Once a requirement for a joint task force (JTF) has been established, the TIOC would be OPCON as the Joint Force Information Operations Component Commander (JFIOCC) to the Commander, Joint Task Force (CJTF). JFQ: "The after action report noted that senior exercise mentors, the joint task force commander, and the combatant commander all agreed that information operations needed a centralized commander to coordinate activities on the JTF level. A joint information operations task force (JIOTF) would fill this need" … "the need for JIOTF as part of a JTF staff is critical to establish and maintain the knowledge superiority needed to execute rapid decisive operations."

[7] The author was a member of the JTF 519 IO Directorate (J39) from January 2005 to June 2007 and a member of the Commander, U.S. Pacific Fleet (COMPACFLT) IO Directorate (N39) from March 2005 to June 2007. During his tenure, the JTF 519 Staff deliberated on the manner in which to Operationally C2 Joint IO and Cyberspace Operations, to include; 1) delegation of C2 to an existing FCC, possibly JFLCC, JFACC, or JMCC, 2) creation of a separate FCC who would be tasked and delegated C2 for IO (and CNO), and 3) retention of C2 of IO (and CNO) by the JTF Commander. During his tenure on the COMPACFLT Staff, the author participated in the construction of Exercise TALISMAN SABER 2007, a Tier II-

Level Joint Exercise, if which JTF 507 (Cmdr, U.S. SEVENTH Fleet) employed a Joint Functional IO Component Commander (JFIOCC) to exercise Operational C2 of IO (and CNO).

[8] Milan N. Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: Naval War College, 2007), IV-3.

[9] The terms medium, environment, domain, and dimension are not specifically defined in current Joint Doctrine as evidenced by a review of the current versions of JP 1-02 (*Department of Defense Dictionary of Military and Associated Terms*, JP 3-0 (*Joint Operations*), and JP 3-13 (*Information Operations*). JP 1-02 provides definitions for maritime domain, space, aerospace, cyberspace, and information environment, but does specifically define the terms medium, environment, domain or dimension.

[10] Department of Defense, *Functions of the Department of Defense and Its Major Components,* Department of Defense (DODD) 5100.1 (Washington, DC: DoD 21 November 2003), 15, 17 and 21. The following are the function of each of the Armed Services: "Department of the Navy: To organize, train, equip and provide Navy and Marine Corps forces for the conduct of prompt and sustained combat incident to operations at sea, including operations of sea-based aircraft and land-based naval air components -- specifically, forces to seek out and destroy enemy naval forces and to suppress enemy sea commerce, to gain and maintain general naval supremacy, to control vital sea areas and to protect vital sea lines of communication, to establish and maintain local superiority (including air) in an area of naval operations, to seize and defend advanced naval bases, and to conduct such land, air, and space operations as may be essential to the prosecution of a naval campaign. Department of the Air Force: To organize, train, equip, and provide forces for the conduct of prompt and sustained offensive and defensive combat operations in the air and space -- specifically, forces to defend the United States against air and space attack in accordance with doctrines established by the JCS, gain and maintain general air and space supremacy, defeat enemy air and space forces, conduct space operations, control vital air areas, and establish local air and space superiority… Department of the Army: To organize, train, and equip forces for the conduct of prompt and sustained combat operations on land -- specifically, forces to defeat enemy land forces and to seize, occupy, and defend land areas."

[11] Luck, Gary, *Insights on Joint Operations: The Art and Science – Best Practices. (*Virginia: U.S. Joint Forces Command, Joint Warfighting Center, 2006), 13-15.

[12] Chairman, U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication (JP) 3-0 (Washington, DC: CJCS, 13 February 2008, II-20 – II-21. Chairman, U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: CJCS, 17 October 2007), 10. "Aerospace — Of, or pertaining to, Earth's envelope of atmosphere and the space above it; two separate entities considered as a single realm for activity in launching, guidance, and control of vehicles that will travel in both entities." "Land" is not formally defined in Joint Doctrine as indicated by a review of the current JP. Chairman, U.S. Joint Chiefs of Staff, *Command and Control of Joint Maritime Operations*, Joint Publication (JP) 3-32 (Washington, DC: CJCS, 8 August 2006, I-2. "Maritime domain — The oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals." Chairman, U.S. Joint Chiefs of Staff, *Joint Doctrine for Space Operations*, Joint Publication (JP) 3-14 (Washington, DC: CJCS, 9

August 2002, GL-5. “Space. A medium like the land, sea, and air within which military activities shall be conducted to achieve US national security objectives.”

[13] Chairman, U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: CJCS, 17 October 2007), 261.

[14] Chairman, U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication (JP) 3-0 (Washington, DC: CJCS, 13 February 2008, II-22.
“The physical dimension - is composed of the C2 systems and supporting infrastructures that enable individuals and organizations to conduct operations across the air, land, maritime, and space domains. It is also the dimension where physical platforms and the communications networks that connect them reside. This includes the means of transmission, infrastructure, technologies, groups, and populations. The informational dimension - is where information is collected, processed, stored, disseminated, displayed, and protected. It is the dimension where C2 of modern military forces is communicated and where commander’s intent is conveyed. It consists of the content and flow of information, and links the physical and cognitive dimensions. The cognitive dimension - encompasses the mind of the decision maker and the target audience. This is the dimension in which commanders and staff think, perceive, visualize, and decide. This dimension also is affected by a commander’s orders, training, and other personal motivations. Battles and campaigns can be lost in the cognitive dimension. Factors such as leadership, morale, unit cohesion, emotion, state of mind, level of training, experience, situational awareness, as well as public opinion, perceptions, media, public information, and rumors influence this dimension.”

[15] Chairman, U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13 (Washington, DC: CJCS, 6 February 2006), GL-6.

[16] Secretary of Defense. *The Quadrennial Defense Review (QDR) Report*, (Washington, DC: The Pentagon, 2006), 23, 37, and 89; and Chairman, U.S Joint Chief of Staff, *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow*, (Washington, DC: The Pentagon, 2004), 1, 5, and 7. QDR: “Capabilities to locate, tag and track terrorists in all domains, including cyberspace.” “Surge – contribute to the nation’s response to and management of the consequences of WMD attacks or a catastrophic event, such as Hurricane Katrina, and also to raise the level of defense responsiveness in all domains (e.g., air, land, maritime, space and cyberspace) if directed.” “Concepts and constructs enabling unity of effort with more than 70 supporting nations under the Proliferation Security Initiative should be extended to domains other than WMD proliferation, including cyberspace, as a priority.” NMS: “The Department must work to secure strategic access to key regions, lines of communication and the “global commons” of international waters, airspace, space and cyberspace.” “Adversaries threaten the United States throughout a complex battlespace, extending from critical regions overseas to the homeland and spanning the global commons of international airspace, waters, space and cyberspace.” “The Armed Forces must have the ability to operate across the air, land, sea, space and cyberspace domains of the battlespace.”

[17] Chairman, U.S. Joint Chiefs of Staff, *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the*, Joint Publication (JP) 2-01.3 (Washington, DC: CJCS, 24 May 2000), II-34.

[18] U.S. Air Force. *Air Force Glossary.* Air Force Doctrine Document (AFDD) 1-2. (Washington, DC: Department of the Air Force, 11 January 2007), 48.

[19] Figures (1) and (2) were developed by the author of this paper and represent his interpretation of the Physical Environment with and without the inclusion of cyberspace.

[20] Milan N. Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: Naval War College, 2007), IV-3.

[21] Ibid., IV-3.

[22] For this discussion, land and maritime forces consider all of their constituent elements less their embedded air platforms - manned and unmanned fixed wing and rotary.

[23] Milan N. Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: Naval War College, 2007), VIII-7.

[24] Ibid., VIII-18.

[25] Chairman, U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: CJCS, 17 October 2007), 101.

[26] Chairman, U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication (JP) 3-0 (Washington, DC: CJCS, 13 February 2008), III-5.

[27] Chairman, U.S. Joint Chiefs of Staff, *Joint Communications System*, Joint Publication (JP) 6-0 (Washington, DC: CJCS, 20 March 2006), GL-7. "Command and control system. The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned and attached forces pursuant to the missions assigned. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)"

[28] Ibid., viii.

[29] Ibid., viii.

[30] Figure (3) was developed by the author of this paper and represents his visualization of the Global Information Grid (GIG).

[31] Milan N. Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: Naval War College, 2007), VIII-18.

[32] Chairman, U.S. Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication (JP) 2-0 (Washington, DC: CJCS, 22 June 2007), V-1.

[33] Chairman, U.S. Joint Chiefs of Staff, *Joint Fires Support*, Joint Publication (JP) 3-09 (Washington, DC: CJCS, 13 November 2006), vii.

[34] Milan N. Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: Naval War College, 2007), VIII-95.

[35] Ibid., VIII-95.

[36] Chairman, U.S. Joint Chiefs of Staff, *Doctrine for Logistic Support of Joint Operations*, Joint Publication (JP) 4-0 (Washington, DC: CJCS, 6 April 2000), I-17.

[37] Chairman, U.S. Joint Chiefs of Staff, *Joint Communications System*, Joint Publication (JP) 6-0 (Washington, DC: CJCS, 20 March 2006), viii-xi. "Commander United States Strategic Command (CDRUSSTRATCOM) has overall responsibility for global network operations (GNO) and defense in coordination with the Chairman of the Joint Chiefs of Staff (CJCS) and the other combatant commands" and "USSTRATCOM was assigned the Unified Command Plan mission to operate and defend the GIG." "CDRUSSTRATCOM has delegated operational and tactical level planning, force execution, and day-to-day

management of the operations and defense of the GIG to the JTF-GNO (Joint Task Force-Global Network Operations)" and "Combatant commanders oversee and coordinate GIG planning and employment within their areas of responsibility," where "they utilize the JTF-GNO, the theater network operations center (TNC) hierarchy, as well as Service component command TNCs as appropriate, and joint control centers." "To this end, they [COMCOMs] collaborate with their respective Service components, Defense Information Systems Agency, Defense Intelligence Agency (DIA), and USSTRATCOM to create and maintain visibility over theater networks." "A Joint Force Commander [i.e. JTF] ensures an adequate and effective communications system is available to support the joint force C2 system" and does this by various actions to include establishing a JNCC [Joint Network Communication Center] to establish network control and management within the operational area." Thus, STRATCOM is managing the GIG, the COCOM is essentially managing the theater portion of the GIG, and the JTF the GIG that is in his Area of Operations.

[38] Chairman, U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication (JP) 3-0 (Washington, DC: CJCS, 13 February 2008), III-1.

[39] U.S. Air Force. *Command and Control.* Air Force Doctrine Document (AFDD) 2-8. (Washington, DC: Department of the Air Force, 1 June 2007), 55 - 56.

[40] Chairman, U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: CJCS, 17 October 2007), 210.

[41] Chairman, U.S. Joint Chiefs of Staff, *Joint Communications System*, Joint Publication (JP) 6-0 (Washington, DC: CJCS, 20 March 2006), A-3.

[42] Ibid., I-10.

[43] Chairman, U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13 (Washington, DC: CJCS, 6 February 2006), II-15.

[44] Ibid., II-5.

[45] Ibid., II-5.

[46] Ibid., II-4.

[47] Ibid., II-4.

[48] Ibid., II-4.

[49] Chairman, U.S. Joint Chiefs of Staff, *Unified Action Armed Services*, Joint Publication (JP) 0-2 (Washington, DC: CJCS, 10 July 2001), V-18.

[50] Chairman, U.S. Joint Chiefs of Staff, *Joint Task Force Headquarters*, Joint Publication (JP) 3-33 (Washington, DC: CJCS, 16 February 2007), III-2 – III-15.

[51] Ibid., III-11 – III-21.

[52] A FCC for Cyberspace Operations is not specifically addressed nor discussed in any of the current Joint Doctrine Publications as evidenced by a review of the current versions of JP 1-02 (*Department of Defense Dictionary of Military and Associated Terms*, JP 3-0 (*Joint Operations*), JP 3-13 (*Information Operations*), and JP 3-33 (*Joint Task Force Headquarters*).

[53] Chairman, U.S. Joint Chiefs of Staff, *Joint Communications System*, Joint Publication (JP) 6-0 (Washington, DC: CJCS, 20 March 2006), II-23.

[54] Chairman, U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13 (Washington, DC: CJCS, 6 February 2006), IV-5.

[55] Chairman, U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: CJCS, 17 October 2007), 568. "Unity of Effort — Coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization - the product of successful unified action."

[56] Milan N. Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: Naval War College, 2007), VIII-13.

[57] Ibid.,VIII-13 thru 14

[58] Ibid., VIII-13.

[59] Chairman, U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: CJCS, 17 October 2007), 393. "Operational control — Command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority) and may be delegated within the command. Operational control is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions; it does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called OPCON. See also combatant command; combatant command (command authority); tactical control."

[60] The author was a member of the JTF 519 IO Directorate (J39) from January 2005 to June 2007 and a member of the COMPACFLT IO Directorate (N39) from March 2005 to June 2007. During his tenure, C2 of CNO in peacetime, contingencies, and crises was a significant topic of discussion and analysis. Several constructs for C2 of CNO for each situation was discussed, which included the following: 1) STRATCOM retaining OPCON of cyberspace forces, 2) STRATOM delegating OPCON of cyberspace forces to the Global Combatant Commander, who would retain OPCON, 3) the GCC delegating OPCON of cyberspace forces to a subordinate JTF Commander, who would retain, and 4) CJTF delegating OPCON for cyberspace forces to an existing FCC (JFMCC, JFACC, etc) or to a Joint FCC for IO. Several of these constructs was exercised annually during TERMINAL FURY (Tier 1-Level exercise for the United States Pacific Command).

[61] Milan N. Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: Naval War College, 2007), VIII-13. Simplicity means that the CoC is clear and straightforward, and "the responsibilities and authority of the operational commander and subordinate commanders [are] clearly delineated." UoE is the "coordination and cooperation toward common objectives" which "can be achieved either through UoC or through cooperation", where "UoC means having a single commander control all forces assigned to a particular mission." Homogeneity means "that all the functions required to accomplish the mission of

the organization should be grouped, and that individuals should be assigned to these groupings in accordance with their abilities.”

BIBLIOGRAPHY

Alexander, Keith B., "Warfighting in Cyberspace." *Joint Forces Quarterly*, no. 46 (3rd Quarter 2007): 58-61.

Howes, Norman R., Mezzino, Michael, and Sarkesian, John, *On Cyber Warfare Command and Control Systems.* Alexandria, VA: Institute for Defense Analyses, 2004.

Joint Chiefs of Staff J7 Joint Education and Doctrine Division. "Joint Doctrine Update." *Joint Forces Quarterly*, no. 49 (2nd Quarter 2008): 6.

Luck, Gary, *Insights on Joint Operations: The Art and Science – Best Practices.* Norfolk, VA: U.S. Joint Forces Command, Joint Warfighting Center, 2006.

Maiers, Mark W., and Rahn, Timothy, L., "Information Operations and Millennium Challenge." *Joint Forces Quarterly*, no. 35 (Autumn 2004): 83-87.

Maney, Kevin. "If U.S. launches cyberattack, it could change nature of war." *USA Today*, 12 February 2003.

Myers, John, M. "Operational Command and Control for Information Operations." Research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2006.

U.S. Air Force. *Air Force Glossary*. AFDD 1-2. Washington, DC: Department of the Air Force, 11 January 2007.

U.S. Air Force. *Command and Control*. AFDD 2-8. Washington, DC: Department of the Air Force, 1 June 2007.

U.S. Department of Defense. *Functions of the Department of Defense and Its Major Components, Department of Defense Directive (DODD)* 5100.1. Washington, DC: DoD, 21 November 2003.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Unified Action Armed Forces*. Joint Publication (JP) 0-2. Washington, DC: CJCS, 10 July 2001.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms*. Joint Publication (JP) 1-02. Washington, DC: CJCS, 17 October 2007.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Intelligence*. Joint Publication (JP) 2-0. Washington, DC: CJCS, 22 June 2007.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*. Joint Publication (JP) 2-01.3. Washington, DC: CJCS, 24 May 2000

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Operations*. Joint Publication (JP) 3-0. Washington, DC: CJCS, 13 February 2008.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Fire Support*. Joint Publication (JP) 3-9. Washington, DC: CJCS, 13 November 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Operations*. Joint Publication (JP) 3-13. Washington, DC: CJCS, 13 February 2006.

U.S Office of the Chairman, of the Joint Chiefs of Staff. *Joint Doctrine for Space Operations*, Joint Publication (JP) 3-14 (Washington, DC: CJCS, 9 August 2002.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Command and Control for Joint Air Operations*. Joint Publication (JP) 3-30. Washington, DC: CJCS, 05 June 2003.

U.S Office of the Chairman, of the Joint Chiefs of Staff. *Command and Control of Joint Land Operations*. Joint Publication (JP) 3-31 (Washington, DC: CJCS, 23 March 2004.

U.S Office of the Chairman, of the Joint Chiefs of Staff. *Command and Control of Joint Maritime Operations*, Joint Publication (JP) 3-32 (Washington, DC: CJCS, 8 August 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Task Force Headquarters*. Joint Publication (JP) 3-33. Washington, DC: CJCS, 16 February 2007.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Doctrine for Logistic Support of Joint Operations*. Joint Publication (JP) 4-0. Washington, DC: CJCS, 6 April 2000.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Communications System*. Joint Publication (JP) 6-0. Washington, DC: CJCS, 20 March 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow*. Washington, DC: CJCS, 2004.

U.S. Office of the Secretary of Defense. *The Quadrennial Defense Review Report*. Washington, DC: SECDEF, 2006.

Vego, Milan, N., Dr., *Operational Warfare*. U.S. Naval War College, Newport, RI: 20

September 2007.

Willard, Robert F., “The Art of Command and Control”, *Proceedings*, October 2002. http://www.military.com/NewContent/0,13190,NI_Art,00.html (accessed 15 March 2008).